分工式门限认证加密方案

谭作文[1),2),3)] 范艳芳[4)]

[1)](江西财经大学信息管理学院计算机系 南昌 330032)

[2)](福建师范大学数学与计算机学院网络安全与密码重点实验室 福州 350007)

[3)](中国科学院软件研究所信息安全重点实验室 北京 100190)

[4)](北京交通大学计算机与信息技术学院 北京 100044)

摘 要 (t,n)门限认证加密方案允许 t 个以上签名方产生指定接收方的认证加密签名,使得只有指定的接收方能够恢复消息和验证消息的完整性,而其他人却无法做到这一点.最近,在 Tseng 和 Jan 的认证加密方案的基础上,Chung 等构造了一个(t,n)门限认证加密方案.该方案运用了分工式签名技术,有效地减轻了签名方的负担.然而,该文作者对该方案的安全性仅进行了解释性说明.目前,文献中没有对分工式门限认证加密的形式化刻画,没有出现可证安全分工式门限认证加密方案.事实上,Chung 等的分工式门限认证加密方案存在设计上的缺陷.文中给出了分工式门限认证加密方案的形式化模型和安全模型,基于双线性映射构造了一个新的分工式门限认证加密方案.在随机预言机模型下,证明了该方案对于适应性选择密文攻击是语义安全的,该方案对于适应性选择消息攻击是存在性不可伪造的.方案的安全性可规约到计算性 Diffie-Hellman(CDH)困难假设和决定性双线性 Diffie-Hellman困难假设(DBDH).

关键词 公钥密码学;门限签名;认证加密方案;随机预言机模型

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.01183

A Division-of-Labor Based Threshold Authenticated Encryption Scheme

TAN Zuo-Wen[1),2),3)] FAN Yan-Fang[4)]

[1)](*Department of Computer, School of Information Technology, Jiangxi University of Finance and Economics, Nanchang* 330032)

[2)](*Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou* 350007)

[3)](*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

[4)](*School of Computer and Information Technology, Beijing Jiaotong University, Beijing* 100044)

Abstract A (t,n) threshold authenticated encryption scheme allows t or more signers to generate a signature on a message for the designated recipient. No one except the designated recipient can recover the message and verify the integrity of the message. Based on Tseng and Jan's authenticated encryption scheme, Chung et al. recently proposed a (t,n) threshold authenticated encryption scheme by applying a division-of-labor signature to reduce the workload of the signers. However, the authors only gave some intuitional security proof. No published paper analyzes formally division-of-labor based threshold authenticated encryption(DOLTAE) scheme in the literature, let alone any proven-secure scheme. As matter of fact, there exists a design defect in the DOLTAE scheme. In this paper, the authors would like to formalize the DOLTAE scheme and its security model. According to the formal model, the authors present a new DOLTAE scheme from bilinear pairings. On the assumptions of Computational Diffie-Hellman (CDH) and Decisional

收稿日期:2009-07-24;最终修改稿收到日期:2010-05-13.本课题得到国家自然科学基金(10961013)资助.**谭作文**,男,1967 年生,博士,副教授,主要研究方向为密码学、信息安全. E-mail: tanzyw@yahoo.com.cn. **范艳芳**,女,1979 年生,博士研究生,主要研究方向为计算机安全、安全模型.

Bilinear Diffie-Hellman (DBDH), the proposed scheme has been proved to be tightly semantically secure against adaptive chosen-ciphertext attacks (IND-CCA2) and existential unforgeable with integrity of ciphertext (UF-CTXT) against the adaptive chosen-message attacks in the random oracle model.

Keywords public key cryptosystem; threshold signature; authenticated encryption scheme; random oracle model

1 引 言

消息的私密性和对消息发送者的认证是开放网络环境下通信的两个基本安全目标.加密方案和签名方案或消息认证码能够分别用来实现上述目标.Nyberg 和 Rueppel[1] 基于离散对数问题提出了第一个具有消息恢复功能的签名方案.在他们的方案中,签名方产生消息的签名后,只有指定的验证者才能恢复消息,认证消息的发送者和验证消息的完整性.这种方案被称作认证加密(authenticated encryption)方案,简称 AE 方案.自从 Nyberg 和 Rueppel 提出第一个 AE 方案以来,已有大量的 AE 方案[2-3]被设计出来.AE 方案能够同时实现消息的私密性和发送方的认证性两个目标.为了给 AE 方案增加更多的安全性能,Nyberg 和 Rueppel[2] 认为构造 AE 方案最好的方式是先签名-后加密(sign-then-encrypt).通过先签名-后加密,签名方能够保证只有指定的消息接受者或验证方才能解密并验证签名.

可证安全是密码学组件设计的一个十分重要的基本要求.Bellare 和 Rogaway 定义[4] 了随机预言机模型(Random Oracle Model,RO 模型).然而,AE 方案一直到 Bellare 和 Namprempre[5] 讨论对称密码系统中的 AE 方案,才有了形式化的安全定义.文献[6]将 AE 方案的认证性分为明文完整性和密文完整性,而将方案的私密性分为选择明文攻击下的不可区分性(IND-CPA)和选择密文攻击下的不可区分性(IND-CCA)以及选择明文攻击下的非延展性(NM-CPA).该文还分析了对称密码方案与消息认证码(MAC)通过常规组合方法构造的 AE 方案的安全性.这些常规组合方法包括加密-MAC(Encrypt-and-MAC)、先 MAC-后加密(MAC-then-encrypt)和先加密-后 MAC(Encrypt-then-MAC).对于每一种构造方法,Bellare 和 Namprempre 讨论了在对称密码方案具有选择明文攻击安全 IND-CPA 和 MAC 具有选择消息安全时,相应 AE 方案的安全性质.此外,文献[5]给出了 AE 方案的安全性质严格证明.对于 AE 方案不具有的安全性质,也给出了反例.

在 2001 年,An[7] 给出了非对称密码系统中 AE 方案形式化的安全定义.文献[7]提出了非对称密码系统下 AE 方案的两个认证概念,这些认证性概念比对称密码系统中 AE 方案的完整性具有更强的密码学意义.与对称密码系统 AE 方案[6] 形成鲜明对照的是,非对称密码系统中的 AE 方案[8] 即使具有选择明文攻击下不可区分性(IND-CPA)和密文完整性(integrity of ciphertext,INT-CTXT),仍无法保证 AE 方案具有抵抗适应性选择密文攻击下的不可区分性(IND-CCA2).An 分别使用 3 种常规组合方法,即加密-签名(Encrypt-and-Sign)、先签名-后加密(Sign-then-Encrypt)和先加密-后签名(Encrypt-then-Sign),把公钥密码加密方案和数字签名方案构造成 AE 方案,并对 3 种 AE 方案的安全性质进行了分析.研究表明:3 种构造方法中没有哪一种方法可以确保相应的 AE 方案具有文献[7]中所定义的所有安全性质.An 还证明了:即使是基于 Diffie-Hellman 的认证加密方案也不能满足下列较强意义的安全性质:抵抗选择明文攻击下接收方密文存在性不可伪造性(receiver existential unforgery with ciphertext forgery,RUF-CTXT)和抵抗选择消息攻击下接收方明文存在性不可伪造性(receiver existential unforgery with plaintext forgery,RUF-PTXT).

另一种可以同时提供认证和保密性的密码学概念是由 Zheng 首次提出来的签密[6].AE 方案和签密方案同时将签名与加密结合起来,但在 AE 方案中加密和认证仅仅使用对称密码系统(对称系统环境中的 AE 方案),或仅仅使用公钥密码系统(非对称系统环境中的 AE 方案).但是,签密方案必须同时使用对称密码系统和公钥密码系统.

基于非对称密码系统的 AE 方案存在一个缺

陷：因为只有指定的接收者才能验证签名的有效性，签名方可能会否定自己所产生的签名. 为了解决这个问题，Araki 等[8]提出了一种可转换认证加密方案（Convertible Authenticated Encryption，CAE）. CAE 方案可以将认证加密的结果转换为一般的数字签名，任何收到签名的参与方都可以验证签名的有效性. 2002 年，Wu 等[9]发现：在 Araki 等的 CAE 方案[8]中，如果签名方不合作，认证加密的结果就不能转换为一般的数字签名. Wu 等提出了一个改进的 CAE 方案[9]. 然而，Huang 和 Chang 发现[10]：在 Wu 等的 CAE 方案中，攻击者如果得到了消息，就能轻易地将认证加密的结果转换为一般的数字签名. Huang 和 Chang 设计了一个新的 CAE 方案[10]，弥补了 Wu 等的 CAE 方案的缺点.

为了降低风险，一个文件常常由两个或更多的签名方来执行签名. 面向群的签名就是这种类型的签名之一. Itakura 与 Nakamura 于 1983 年应用面向群的签名构造了多重签名方案[11]. 然而文献[8-10]中的 CAE 方案并不适合存在多签名方的情形. Wu 等构造了一个有消息冗余的可转换多重认证加密方案[12]（Convertible Multi-Authenticated Encryption，CMAE）. Tsai 运用单向杂凑函数构造了基于离散对数问题的高效 CMAE 方案，消除了消息冗余[13].

门限签名[14-15]是另一种类型的面向群的签名. 这种签名常常需要运用密钥共享技术，n 个参与者组成的团体中，任意 t 个或 t 个以上参与者可以代表整个团体对消息签名，而少于 t 个不能够代表整个团体对消息签名. Chen 等应用门限签名构造一个门限 AE 方案（Threshold Authenticated Encryption，TAE）[16].

对 AE 方案的研究方向除了形式化安全证明外，还有如何提高 AE 方案的效率[3,17-18]. 尽管在签名方案中使用消息的 Hash 值能够有效减少签名大小，但在 AE 方案中却不能使用该技术，因为必须从密文中恢复消息. 签密也许更适合于传输较长的消息. 然而，签密需同时使用对称密码系统和非对称密码系统. 因此，在设计 AE 方案时，一些研究者利用分工式技术将较长的消息分成若干短消息块，每个消息块附有前一个消息块的链接信息和产生前一个消息块签名的秘密信息[17-18]. 最近，Chung 等基于门限密码系统[19]和 Tseng 与 Jan 的 AE 方案[20]，借助于分工式技术构造了一个 (t,n) 门限 TAE 方案[21]，该方案中每个消息块附有前一个消息块的链接信息. 分工式技术的主要思想是：整个消息先被分成若干消息块，每个签名参与者分配到其中一个消息块，每个签名参与者只对自己的消息块进行认证加密，最后将所有子密文组合成整个消息的面向群的密文. 为了简单起见，下文称 Chung 等的 TAE 方案[21]为 CHC-DOLTAE 方案.

Boneh、Lynn 和 Shacham 设计了一个基于双线性映射的高效率短签名方案（BLS）[22]. 该签名方案基于计算性 Diffie-Hellman（CDH）假设在 RO 模型中是可证安全的.

本文的主要贡献是：

CHC-DOLTAE 方案[21]使用分工式签密技术处理较长消息，能够有效地减少每一个签名方的工作负担，所采用的 TAE 方案里的门限策略能改善 AE 方案面向群的安全性. 但是，本文分析发现 CHC-DOLTAE 方案存在着设计上的缺陷. 而且，文献[21]仅对 CHC-DOLTAE 方案安全性质做了解释性说明. 可证安全性是密码协议设计时不可缺少的要求. 在形式化的模式下设计安全分工式门限认证加密方案（Division-Of-Labor based Threshold Authenticated Encryption，DOLTAE）是一个有趣的问题. 对于公钥认证加密（PKAE）方案的安全性，仅仅考虑方案能够抵抗接收方攻击和第三方攻击下适应性选择密文攻击就足够了. 然而，对于 TAE 方案，其安全性并不尽相同. 因为对于 TAE 方案，敌手也许来自第三方、接收方或者 $t-1$ 个签名参与方，甚至可以是 $t-1$ 个签名参与方与接收方组成的合谋团体. 在 TAE 方案中，恶意的接收方可能与一部分签名方合谋伪造有效密文，而只需要求参与合谋的签名方数目少于门限值. 在上述敌手中，最后一种敌手具有最强大的攻击能力. 在本文中，将讨论 DOLTAE 在接收方与 $t-1$ 个签名参与方合谋攻击模式下适应性选择消息攻击的保持密文完整的不可伪造性（Unforgeability with ciphertext integrity，UF-CTXT）. 这样把 TAE 方案认证安全从文献中较强意义下的 RUF-CTXT 扩展到最强意义下的 UF-CTXT.

在 BLS 方案的基础上，我们设计了一个具体的 DOLTAE 方案. 新的 DOLTAE 方案被证明：基于 CDH 和 DBDH（Decisional Bilinear Diffie-Hellman）假设，在 RO 模型中，具有抵抗适应性选择密文攻击紧致不可区分性（IND-CCA2）和抵抗适应性选择消息攻击保持密文完整的不可伪造性（UF-CTXT）.

此外，从本文构造的 DOLTAE 方案，很容易

构造出多重认证加密方案(Multi-Authentication Encryption,MAE)或 TAE 方案.

本文第 2 节给出部分预备知识;第 3 节简单回顾一下 CHC-DOLTAE 方案;DOLTAE 方案的形式化模型在第 4 节给出;第 5 节描述新的 DOLTAE 方案;第 6 节分析新方案的安全性;最后是全文的总结.

2 预备知识

在这一节,回顾一下双线性映射和一些密码学假设.

2.1 记 号

首先介绍本文将要使用到的一些记号. 令$\mathcal{U}=\{U_1,U_2,\cdots,U_n\}$表示 n 个签名方组成的签名方群,U_i表示第 i 个签名方($i=1,2,\cdots,n$).$\mathcal{U}_a$表示实际签名参与者组成的签名方群,U_r是密文接收方,U_c是实际签名方群$\mathcal{U}_a$中的签名收集者,U_c可以是$\mathcal{U}_a$中的任何一个签名方. 用 $Ind(SET)$ 表示指标集$\{i\,|U_i\in SET\}$.

2.2 双线性映射

G_1与 G_2是两个素数 p 阶循环群,g 是群 G_1的一个生成元. e 是一个从 $G_1\times G_1$到 G_2的可容许映射,该映射满足下列性质:

(1)双线性. 对于任意 $u,v\in G_1,a,b\in Z_p^*$,均有 $e(u^a,v^b)=e(u,v)^{ab}$.

(2)非退化. $e(g,g)\neq 1$.

(3)可计算性. 对于任意 $u,v\in G_1$,均存在有效算法计算 $e(u,v)$.

2.3 密码学假设

定义 1(DBDH 问题). 已知循环群 G_1中四元组(g,g^a,g^b,g^c),其中 $a,b,c\in Z_p^*$ 为未知的指数,对于 $Z\in G_2$,判断 $Z=e(g,g)^{abc}$是否成立.

一个能求解 DBDH 问题的概率多项式时间区分器 A 具有的优势定义如下:

$$Succ_{A,G_1}^{\mathrm{DBDH}}=|Pr[A(g^a,g^b,g^c,e(g,g)^{abc})=1]-Pr[A(g^a,g^b,g^c,e(g,g)^z)=1]|.$$

定义 2(DBDH 假设). 已知循环乘法群 G_1中四元组(g,g^a,g^b,g^c),其中 $a,b,c\in Z_p^*$ 为未知的指数,对于 $Z\in G_2$,求解 DBDH 问题的概率多项式时间区分器 A 具有的优势是可以忽略的.

定义 3(CDH 问题). 已知循环乘法群 G_1中三元组(g,g^a,g^b),其中 $a,b\in Z_p^*$ 为未知的指数,计算 g^{ab}.

一个能求解 CDH 问题的概率多项式时间算法 A 具有的优势定义如下:

$$Succ_{A,G_1}^{\mathrm{CDH}}=Pr[A(g^a,g^b)=g^{ab},a,b\in Z_q^*].$$

定义 4(CDH 假设). 已知循环乘法群 G_1中三元组(g,g^a,g^b),其中 $a,b\in Z_p^*$ 为未知的指数,求解 CDH 问题的概率多项式时间算法 A 具有的优势 $Succ_{A,G_1}^{\mathrm{CDH}}$是可以忽略的.

定义 5(DDH 问题). 已知循环乘法群 G_1中四元组(g,g^a,g^b,g^c),其中 $a,b,c\in Z_p^*$ 为未知的指数,判断 $g^{ab}=g^c$是否成立.

如果存在可容许映射 $e:G_1\times G_1\to G_2$,那么 G_1中的 DDH 问题很容易通过 $e(g^a,g^b)=e(g,g^c)$来解决.

定义 6(GDH 群). 如果群 G_1中的 CDH 问题是难解的,而 DDH 问题容易求解,就称 G_1是 GDH 群(Gap Diffie-Hellman Group).

3 CHC-DOLTAE 方案回顾

为了更好地理解分工式认证加密技术,在这一节先回顾一下 CHC-DOLTAE 方案[21],然后对该方案的安全性做简要分析. CHC-DOLTAE 方案[21]在椭圆密码系统[23]和 DOLTAE 方案[16]的基础上运用了消息链接技术和分工式签名技术. 在 CHC-DOLTAE 方案中,签名群$\mathcal{U}$中的每个签名方 U_i具有公开信息 x_i. 根据实际签名方子群中的参与者数目如 t 个,将每个较长的消息分成 t 个消息块,然后给每个签名参与者分配一个消息子块. 实际签名方子群中的参与者只需要对分配给他的消息子块签名. CHC DOLTAE 方案包含 3 个阶段.

系统初始化阶段. 系统可信方 SA 选择大素数 p 和 q,有限域 F_p,F_p上椭圆曲线 E 的 q 阶点群 $E(F_p)$和 $E(F_p)$的一个生成元 P. 设 $h()$是一个公开的单向杂凑函数. SA 通过下列方式产生方案各个参与者的私钥.

(1)在多项式环 $F_p[x]$中随机选择一个$(t-1)$次多项式:

$$f(x)=e_0+e_1x+e_2x^2+\cdots+e_{t-1}x^{t-1} \quad (1)$$

(2)将 e_0作为签名方群$\mathcal{U}$的私钥,计算 $Y_s=e_0P$ 作为它的公钥.

(3)对于签名方群$\mathcal{U}$中的每个签名方 U_i($i=1,2,\cdots,n$),计算私钥 $f(x_i)$和公钥 $Y_i=f(x_i)P$.

(4)在 Z_q^*中随机选择 x_r作为接受方 U_r的私钥,计算 U_r的公钥 $Y_r=x_rP$.

认证签名产生阶段. 不失一般性，假设实际签名方子群$\mathcal{U}_a$是由 t 个签名方组成$\{U_i \mid i=1,2,\cdots,t\}$. 签名方子群$\mathcal{U}_a$要认证加密消息 M. $\mathcal{U}_a$中 t 个签名方合作将消息 M 分成 t 个相关联的消息块$\{M_1,M_2,\cdots,M_t\}$. 不妨设 $M_i \in Z_p^*$. 为了抵抗文献[24]中的伪造攻击，每个消息块 M_i 均附有消息冗余. 每个签名参与者 U_i 分别对分配给自己的消息块 M_i 通过下列步骤产生签名.

(1) 在 F_q^* 中随机选择一个元素 b_i，计算

$$B_i=b_iP=(x_{B_i},y_{B_i}).$$

(2) 计算 $z_i=(b_i \cdot x_{B_i})Y_r=(x_{z_i},y_{z_i})$.

(3) 通过安全信道将 B_i 和 z_i 发送到$\mathcal{U}_a$中的其他签名参与者.

(4) 收到其他签名参与者发送来的$(B_i,z_i)(i=1,2,\cdots,t)$后，计算 B 和 V：

$$B=\sum_{i=1}^{t}B_i=(x_B,y_B),\ V=\sum_{i=1}^{t}z_i=(x_V,y_V) \quad (2)$$

(5) 计算消息块 M_i 的子密文(r_i,s_i)，并在实际签名方子群$\mathcal{U}_a$中发布子密文：

$$r_i=M_i h(i \parallel x_V) \bmod p,$$

$$s_i=x_{B_i} \cdot b_i-r_i \cdot f(x_i) \cdot \prod_{j=1,j\neq i}^{t}\frac{0-x_j}{x_i-x_j} \bmod q \quad (3)$$

当签名收集者 U_c 收到子密文(r_i,s_i)时，$i=1,2,\cdots,t$，U_c先验证其有效性：

$$x_{B_i}B_i \stackrel{?}{=} s_iP+\left(r_i \cdot \prod_{j=1,j\neq i}^{t}\frac{0-x_j}{x_i-x_j}\right)y_i \quad (4)$$

如果对于 $i=1,2,\cdots,t$，上述等式都成立，则 U_c 将所有子密文组合成整个消息 M 的密文.

$$r=\sum_{i=1}^{t}r_i,\ s=\sum_{i=1}^{t}s_i \quad (5)$$

最后，U_c发送密文$(r,s,r_1,r_2,\cdots,r_t)$给指定的接收方 U_r.

消息恢复阶段. U_r收到签名$(r,s,r_1,r_2,\cdots,r_t)$后，执行下列步骤恢复消息.

(1) 计算与实际签名方群$\mathcal{U}_a$共享会话密钥 V.

$$V=sY_r+(r \cdot x_r)Y_s=(x_V,y_V) \quad (6)$$

(2) 对于 $i=1,2,\cdots,t$，逐个恢复消息块$\{M_1,M_2,\cdots,M_t\}$

$$M_i=r_i \cdot h(i \parallel x_V)^{-1} \bmod p \quad (7)$$

(3) 通过每个消息块附有的冗余信息判别消息块的有效性. 如果所有消息块都是有效的，U_r 获取整个消息 M.

文献[21]给出了 CHC-DOLTAE 安全性质的解释性说明. 因此，其安全性分析不是令人信服的. 分析发现：CHC-DOLTAE 存在着设计缺陷，等式(6)不会成立. 文献[21]中定理 1 的证明是错误的. 因此，密文的接收方 U_r 不可能通过等式(7)恢复消息子块 $M_i(i=1,2,\cdots,t)$. 事实上，

$$\begin{aligned}V&=\sum_{i=1}^{t}z_i=(x_V,y_V)=\sum_{i=1}^{t}(x_{B_i}b_i)Y_r\\&=\sum_{i=1}^{t}(s_i+r_i \cdot f(x_i) \cdot L_i)Y_r\\&=\Big[\sum_{i=1}^{t}s_i+\sum_{i=1}^{t}(r_i \cdot f(x_i) \cdot L_i)\Big]Y_r\\&\neq sY_r+[r \cdot f(0)]Y_r=sY_r+(r \cdot x_r)Y,\end{aligned}$$

上式中，L_i 是 Lagrange 系数.

4　DOLTAE 方案形式化

在这一节，给出形式化 DOLTAE 方案，建立 DOLTAE 方案的安全模型.

4.1　DOLTAE 方案的组成

在 DOLTAE 方案中，有 3 个参与方：签名方群 $\mathcal{U}=\{U_1,U_2,\cdots,U_n\}$，实际参与签名方群$\mathcal{U}_a$和指定接收方 U_r. 一个 DOLTAE 方案由 5 个算法$\{K_c,K_s,K_r,E,D\}$组成.

(1) Setup K_c. 输入安全参数 k，随机算法 K_c 输出系统参数 I. 记作：$I \leftarrow K_c(k)$.

(2) SenderKeyGen K_s：输入系统参数和门限值(n,t)，随机算法 K_s 输出签名方群$\mathcal{U}$ 以及每个签名方公私钥对(pk_U,sk_U)，(pk_{s_i},sk_{s_i}). 记作

$$((pk_U,sk_U),(pk_{s_1},sk_{s_1}),\cdots,(pk_{s_n},sk_{s_n})) \leftarrow K_s(I,(n,t)).$$

(3) ReceiverKeyGen K_r. 输入系统参数，随机算法 K_r 输出指定接收方 U_r 的公私钥对(pk_r,sk_r). 记作$(pk_r,sk_r) \leftarrow K_r(I)$.

(4) DOLTAE E. 输入签名方群$\mathcal{U}$ 的公钥 pk_U，实际参与签名方的私钥 sk_{s_i} 和接收方 U_r 的公钥 pk_r 以及消息 M，随机算法 DOLTAE E 先将消息 M 分为与实际参与签名方数目相同的消息子块，然后产生相应的子密文，最后输出密文 C. 记作 $C \leftarrow E_{\langle pk_U,sk_{s_i}(\forall U_i \in \mathcal{U}_a),pk_r\rangle}(M)$.

(5) DOLTAE D. 输入接收方 U_r 的私钥 sk_r，签名方群$\mathcal{U}$ 的公钥 pk_U，接收方 U_r 的公钥 pk_r 和密文 C，确定性算法 DOLTAE D 输出(pk,M)或符号$\perp$，pk 是发送方公钥，M 是跟密文对应的明文，符号$\perp$表示密文是无效的. 对于解密算法要求：$D_{sk_r}(E_{\langle sk_U,pk_U,pk_r\rangle}(M))=(pk_U,M)$. 记作 $string \leftarrow$

$D_{sk_r}(C)$，$string$ 是⊥或者(pk,M).

4.2 DOLTAE 方案的安全性

在这一小节，定义 DOLTAE 方案的安全性. 安全的 DOLTAE 方案应该同时满足 PKAE[7] 的安全性和门限方案的安全性. 一个 DOLTAE 方案所能满足的最强意义的安全性质是 IND-CCA2 安全和 UF-CTXT 安全.

定义 7(鲁棒性). 对于任意至多能够腐蚀 t 个签名方的概率多项式时间攻击者，DOLTAE 方案(K_c,K_s,K_r,E,D)都能成功地运行.

定义 8(私密性). 设(K_c,K_s,K_r,E,D)是一个 DOLTAE 方案. 令 $b\in\{0,1\}$，k 是系统的安全参数. $E_{\langle pk_U,sk_{s_i}(\forall U_i\in\boldsymbol{U_a}),pk_r\rangle}(\cdot)$是一个 DOLTAE 加密随机预言机(Oracle). 输入一个消息，该 Oracle 返回一个密文. $D_{sk_r}(\cdot)$是一个 DOLTAE 解密随机预言机，输入密文，$D_{sk_r}(\cdot)$返回(pk,M). 设 A 为任意概率多项式时间敌手. 敌手 A 可以询问 DOLTAE 加密随机预言机 $E_{\langle pk_U,sk_{s_i}(\forall U_i\in\boldsymbol{U_a}),pk_r\rangle}(\cdot)$和 DOLTAE 解密随机预言机 $D_{sk_r}(\cdot)$.

考虑下列游戏(game).

(1) 初始化阶段. 运行 Setup 算法 K_c 和 SenderKeyGen 算法 K_s，产生系统参数 I、签名方群$\boldsymbol{U}$ 的公私密钥对(pk_U,sk_U)、签名方的公私密钥对$(pk_{s_i},sk_{s_i})(i=1,2,\cdots,n)$. 运行随机算法 K_r，产生接收方 U_r 的公私密钥对(pk_r,sk_r). 发送$\{I,pk_U,pk_r,pk_{s_i}(i=1,2,\cdots,n)\}$给敌手 A.

(2) 攻击阶段 1. 敌手 A 适应性地作 DOLTAE 加密随机预言机和 DOLTAE 解密随机预言机询问.

DOLTAE 加密随机预言机询问. A 选择一个消息 M，然后作 DOLTAE 加密询问，随机预言机 $E_{\langle pk_U,sk_{s_i}(\forall U_i\in\boldsymbol{U_a}),pk_r\rangle}(\cdot)$做出应答.

DOLTAE 解密随机预言机询问. A 对于 DOLTAE 密文 C 作解密询问，解密随机预言机 $D_{sk_r}(\cdot)$做出应答，返回(pk,M)或者密文无效符号⊥.

(3) 挑战阶段. A 随机选择两个长度相同的消息 M_0 和 M_1. DOLTAE 加密算法先掷一个硬币决定 M_b，$b\in\{0,1\}$，然后加密 M_b，将 DOLTAE 密文 C 返回给敌手 A，作为一个挑战(challenge).

(4) 攻击阶段 2. A 如攻击阶段 1 一样适应性地作 DOLTAE 加密和解密随机预言机询问，但是 A 不被允许关于挑战(challenge)询问 DOLTAE 解密随机预言机.

(5) 猜测阶段. 在游戏结束时，A 输出一个比特 b'. 若 $b'=b$，则 A 在游戏中获胜.

定义敌手 A 在上述游戏中的优势如下

$$Adv^{\text{IND-CCA}}_{\text{DOLTAE},A}(k)=|Pr(b'=b)-1/2| \quad (8)$$

称一个 DOLTAE 方案(K_c,K_s,K_r,E,D)是 IND-CCA 安全，如果不存在概率多项式时间(PPT)敌手以不可忽略的优势在上述游戏中获胜.

尽管 PKAE 方案存在形式化的安全概念，但 TAE 还没有正式的不可伪造性安全概念. 对于 PKAE 方案，敌手 A 可能来自不同于签名方的任何一方，如第三方或者指定的接收方. 因为密文是根据签名方的密钥和接收方的公钥生成的，潜在的敌手分成两类：第三方或者指定的接收方. 一个安全的 PKAE 方案在接收方攻击或第三方攻击模式下能够抵抗适应性选择密文攻击，是不可伪造的[7]. TAE 方案的安全性跟上面的不尽相同. 因为在 TAE 方案中，敌手来自于第三方、接收方、至多$(t-1)$个签名方或者至多$(t-1)$个签名方与接收方的合谋团体. 在门限情形下，只要签名方数目少于门限值，恶意接收方可能与一部分签名方合谋来伪造有效的密文. 在以上所有敌手中，最后一种敌手是最强大的. 在本文中，仅仅讨论 DOLTAE 方案在最强意义下的安全性，即在接收方和$(t-1)$个签名方的合谋攻击模式下适应性选择消息攻击的安全性(UF-CTXT). 敌手的伪造分为两种类型：密文伪造(CTXT)和明文伪造(PTXT). 密文伪造是指敌手产生的密文不同于 DOLTAE 加密随机预言机所产生的密文，而明文伪造是指敌手伪造的密文所对应的明文不同于敌手询问 DOLTAE 加密随机预言机时所使用的明文. DOLTAE 方案抵抗密文伪造的不可伪造性类比了普通数字签名在较强意义下的安全性. 结合合谋攻击下密文不可伪造性，DOLTAE 方案有一个最强意义下的安全性概念：UF-CTXT. 在 DOLTAE 方案的这种安全模型中，敌手可以进行选择消息攻击和密钥改变攻击. DOLTAE 方案的 UF-CTXT 安全定义如下.

定义 9(不可伪造性). 设 DOLTAE 方案为(K_c,K_s,K_r,E,D). k 是安全参数. 假设敌手 F 能访问 DOLTAE 加密随机预言机 $E_{\langle pk_U,sk_{s_i}(\forall U_i\in\boldsymbol{U_a}),pk_r\rangle}(\cdot)$.

考虑以下游戏.

(1) 初始化阶段. 运行 Setup 算法 K_c 和 SenderKeyGen 算法 K_s，产生系统参数 I、签名方群$\boldsymbol{U}$ 的公私密钥对(pk_U,sk_U)、签名方的公私密钥对$(pk_{s_i},sk_{s_i})(i=1,2,\cdots,n)$. 然后，将$\{I,pk_U,pk_r,pk_{s_i}(i=1,2,\cdots,n)\}$发送给敌手 F. F 选择不多于 t 个签名

方作为腐蚀对象，获取他们的公私钥. 甚至允许 F 运行随机算法 K_r，获得接收方的公私钥(pk_r, sk_r).

(2) 攻击阶段. F 适应性地作 DOLTAE 加密随机预言机询问.

DOLTAE 加密随机预言机询问. F 选择消息 M，然后作加密询问，随机预言机 $E_{\langle pk_U, sk_{s_i}(\forall U_i \in \mathbf{U}_a), pk_r\rangle}(\cdot)$ 做出应答.

(3) 密文伪造. 在游戏结束时，敌手 F 产生一个 DOLTAE 密文(C, pk_r', sk_r').

(4) 输出：运行算法 AuthDec D：

$$string \leftarrow D_{sk_r'}(C).$$

① 若 $string$ 是$\perp$，则 F 在游戏中失败. 返回 0.

② 将 $string$ 分组成(pk, M). 若 $pk = pk_U$，密文 C 不是 DOLTAE 加密随机预言机的应答，则 F 在游戏中获胜. 返回 1.

③ 若 $pk \neq pk_U$，则 F 在游戏中失败. 返回 0.

④ 若 C 是 DOLTAE 加密随机预言机的应答，则 F 在游戏中失败. 返回 0.

定义敌手 F 在上述游戏中的优势如下

$$Adv_{\text{DOLTAE},F}^{\text{UF-CTXT}}(k) = Pr(\text{返回值} = 1) \tag{9}$$

称一个 DOLTAE 方案(K_c, K_s, K_r, E, D)是 UF-CTXT 安全，如果不存在 PPT 敌手以不可忽略的优势在上述游戏中获胜.

5　新的 DOLTAE 方案

在这一节，描述一个新的 DOLTAE 方案. 新的 DOLTAE 方案涉及 3 个参与方：签名方群 $\mathbf{U} = \{U_1, U_2, \cdots, U_n\}$，实际参与签名方群 $\mathbf{U}_a$ 和指定接收方 U_r. DOLTAE 方案由以下 5 个算法$\{K_c, K_s, K_r, E, D\}$组成.

Setup K_c. 输入安全参数 k，随机算法 K_c 输出系统参数 $I = \{G_1, G_2, e, g, p, H_1(), H_2()\}$. 其中 G_1 与 G_2 是两个素数 p 阶循环群，g 是群 G_1 的一个生成元. e 是一个从 $G_1 \times G_1$ 到 G_2 的双线性映射，$H_1()$：$\{0,1\}^* \rightarrow G_2$ 和 $H_2()$：$\{0,1\}^* \rightarrow G_1$ 两个安全的杂凑函数.

SenderKeyGen K_s. 随机算法 K_s 采用 Gennaro 等设计的基于离散对数假设分布式密钥生成协议 DKG[25]. 签名方群 $\mathbf{U}$ 中所有成员$\{U_1, U_2, \cdots, U_n\}$共同执行此算法. 输入系统参数 I 和门限值 t，K_s 输出签名方群 $\mathbf{U}$ 的公钥 y. U_i 的私钥 $x_i \in Z_p^*$，并且$\{x_1, x_2, \cdots, x_n\}$是 U 的秘钥 x 依照秘密共享策略所产生的 n 个份额，$x = \log_g y$. 任何 t 个秘钥子集 SET 通过拉格朗日插值法可以重构 $x = \sum_{i \in SET} L_i x_i$，其中 L_i 是 Lagrange 系数. 对每个秘密份额 x_i，计算 $y_i = g^{x_i}$ 作为 U_i 的公钥. 公钥在签名方群 $\mathbf{U}$ 中广播.

ReceiverKeyGen K_r. 给定系统参数 I，随机算法 K_r 选择 $a, b, c \in Z_p^*$ 作为 U_r 的私钥. 计算 $g_1 = g^a$，$g_2 = g^b$，$g_3 = g^c$. K_r 输出指定接收者 U_r 的公钥 $\{g, g_1, g_2, g_3\}$.

DOLTAE E. 不失一般性，假设实际签名方群 $\mathbf{U}_a$ 是由$\{U_i \mid i = 1, 2, \cdots, t\}$组成. $\mathbf{U}_a$ 中的签名方通过执行以下步骤合作生成消息 M 的 DOLTAE 密文.

(1) 消息分块. 明文 M 被分成 t 个消息块. 不妨设第 i 个消息块分给 U_i. 如文献[22]中所示，很容易构造一个将消息映射到 G_2 中点的算法 MapToGroup. 为叙述简便，设 $M_i \in G_2 (i = 1, 2, \cdots, t)$.

(2) 子密文生成. 设 n_i 是消息子块 M_i 的序列号. 每个 U_i 随机选择 $k_i \in Z_p^*$，计算消息子块 M_i 的子密文，在实际签名方群 $\mathbf{U}_a$ 中广播(C_{i1}, C_{i2}, C_{i3})：

$$C_{i1} = g^{k_i},\ \alpha_i = H_1(C_{i1}),$$
$$C_{i2} = Z^{k_i}(n_i \parallel y \parallel M_i),\ C_{i3} = (g_1^{\alpha_i} g_3)^{k_i} \tag{10}$$

接着，u_i 计算

$$s_i = H_2(y \parallel C_{11} \parallel C_{12} \parallel C_{13} \parallel \cdots \parallel C_{t1} \parallel C_{t2} \parallel C_{t3})^{L_i x_i} \tag{11}$$

(3) 子密文有效性验证. U_i 发送子密文$(C_{i1}, C_{i2}, C_{i3}, s_i)$给收集者 U_c，U_c 可以是实际签名方群中的任意签名方. U_c 通过检查下列等式是否成立来验证子密文的有效性：

$$e(g, s_i) = e(y_i, H_2(y \parallel C_{11} \parallel C_{12} \parallel C_{13} \parallel \cdots \parallel C_{t1} \parallel C_{t2} \parallel C_{t3} \parallel)^{L_i}) \tag{12}$$

(4) 密文合成. 如果所有子密文$(C_{i1}, C_{i2}, C_{i3}, s_i)(i = 1, 2, \cdots, t)$都是有效的，$U_c$ 把所有的子密文组合成整个消息 M 的 DOLTAE 密文.

$$s = \prod_{i \in Ind(\mathbf{U}_a)} s_i \tag{13}$$

U_c 通过公共信道将 DOLTAE 密文$(C_{11}, C_{12}, C_{13}, \cdots, C_{t1}, C_{t2}, C_{t3}, s)$发送给指定接收者 U_r.

DOLTAE D：当 U_r 得到密文$(C_{11}, C_{12}, C_{13}, \cdots, C_{t1}, C_{t2}, C_{t3}, s)$时，$U_r$ 执行以下操作.

1. 若有

$$e(g, s) \neq e(y, H_2(y \parallel C_{11} \parallel C_{12} \parallel C_{13} \parallel \cdots \parallel C_{t1} \parallel C_{t2} \parallel C_{t3})),$$

则 U_r 输出$\perp$；否则，执行步 2；

2. U_r 计算 $\alpha_i^* = H_1(C_{i1})$. 若存在某个 $i \in \{1, 2, \cdots, t\}$，有 $C_{i3} \neq C_{i1}^{a\alpha_i^* + c}$，$U_r$ 输出$\perp$；否则，执行步 3；

3. U_r 计算 $string_i^* = C_{i2} / e(C_{i1}, g^{ab})$，将其分组为

$A_i^* \| B_i^* \| M_i^*$. 若 $A_i^* \notin \{1,2,\cdots,t\}$，或 $\exists i \neq j, A_i^* = A_j^*$，或 $\exists i, B_i^* \neq y$，则 U_r 输出 $\perp$；否则，执行步 4；

4. U_r 按照消息子块的序列号 A_i^* 将所有消息块 M_i^* 组合成整个消息 M.

从以上可知，新的 DOLTAE 方案很容易转换为一个 MAE 方案或 TAE 方案. 为简便起见，这里省略转化过程.

6 新的 DOLTAE 方案分析

本节中，将证明新的 DOLTAE 方案基于 CDH 假设是鲁棒的，IND-CCA2 安全和 UF-CTXT 安全的.

定理 1(鲁棒性). 即使存在允许腐蚀少于 $n/2$ 个签名方的 PPT 攻击者，新的 DOLTAE 方案也能够成功地执行. 因此，接收方 U_r 能够恢复整个消息 M.

证明. 如文献[14]所示，即使攻击者腐蚀签名方群 $\mathcal{U}$ 中的少于 $n/2$ 个签名方，任何 t 个份额的集合能够唯一确定对应公钥 y 的私钥 x，并且 x 在 Z_p^* 中是均匀分布的. 因此，y 在 G_1 中也是均匀分布的. 这意味着新的 DOLTAE 方案即使有腐蚀能力的攻击者存在，也能成功地执行.

其次，因为每个有效的 s_i 是对应于公钥 $y_i = g^{x_i}$ 的一个短 BLS 签名[22]，只有有效的 s_i 才能通过验证方程(12). 事实上，有

$$\begin{aligned} & e(g, s_i) \\ &= e(g, H_2(y \| C_{11} \| C_{12} \| C_{13} \| \cdots \| C_{t1} \| C_{t2} \| C_{t3} \|)^{L_i x_i}) \\ &= e(y_i, H_2(y \| C_{11} \| C_{12} \| C_{13} \| \cdots \| C_{t1} \| C_{t2} \| C_{t3} \|)^{L_i}) \end{aligned} \tag{14}$$

密文 s 是通过至少 t 个有效的形如 $H_2(\,)^{L_i x_i}$ 的子密文 s_i 相乘得到的. 依据式子(10)，有

$$C_{i3}^* = (g_1^{\alpha_i^*} g_3)^{k_i} = (g^{aa_i + c})^{k_i} = C_{i1}^{aa_i + c} = C_{i3} \tag{15}$$

因此，通过式子(13)，能够得到

$$\begin{aligned} & e(g, s) = e\Big(g, \prod_{i \in \mathcal{U}_a} s_i\Big) = \prod_{i \in \mathcal{U}_a} e(g, s_i) \\ &= e\Big(\prod_{i \in \mathcal{U}_a} y_i^{L_i}, H_2(y \| C_{11} \| C_{12} \| C_{13} \| \cdots \| C_{t1} \| C_{t2} \| C_{t3} \|)\Big) \\ &= e\Big(g^{\sum_{i \in \mathcal{U}_a} L_i x_i}, H_2(y \| C_{11} \| C_{12} \| C_{13} \| \cdots \| C_{t1} \| C_{t2} \| C_{t3} \|)\Big) \\ &= e(y, H_2(y \| C_{11} \| C_{12} \| C_{13}^* \| \cdots \| C_{t1} \| C_{t2} \| C_{t3}^* \|)). \end{aligned}$$

证毕.

定理 2(私密性). 新的 DOLTAE 方案在 RO 模型下基于 DBDH 假设是 IND-CCA2 安全的，而且有

$$\varepsilon \leq Succ_{A,G_1}^{\mathrm{DBDH}} + \frac{2q_d t}{p} + t\varepsilon_1 + q_d \varepsilon_2,$$

式子中 ε 是攻击者攻破 DOLTAE 方案所具有的优势，$Succ_{A,G_1}^{\mathrm{DBDH}}$ 是求解 DBDH 问题成功的优势，ε_1 是杂凑函数 $H_1(\,)$ 的目标碰撞概率，ε_2 是伪造有效 BLS 签名成功的概率，t 是门限值，q_d 是解密随机预言机访问的次数，且 $q_d \leq p/2$.

证明. 假设存在一个 (t_1, ε) 的攻击者 A. 敌手 A 在时间 t_1 内以概率 ε 攻破新的 DOLTAE 方案. 那么，能够构造一个算法 B 在时间 t_2 内以优势 $Succ_{A,G_1}^{\mathrm{DBDH}}$ 求解 DBDH 问题的一个随机实例.

G_1 与 G_2 是两个素数 p 阶循环群，g 是群 G_1 的一个生成元. 给算法 B 输入 5 元组 $(g, g^a, g^b, g^{k^*}, Q^*) \in G_1^4 \times G_2$. 当 $Q^* = e(g,g)^{abk^*}$ 时，算法 B 输出 1；当 $Q^* \neq e(g,g)^{abk^*}$ 时，算法 B 输出 0. 算法 B 与敌手 A 交互进行下列游戏.

初始化阶段. 算法 B 运行 K_c. 输入安全参数 k，K_c 如第 5 节方案中一样输出系统参数 $I = \{G_1, G_2, e, p, H_1(\,), H_2(\,)\}$. 算法 B 运行算法 K_s. 把系统参数 I 和门限值 t 作为 K_s 的输入. 算法 B 随机选择一个私钥 $x_i \in Z_p^*$ 作为签名方 U_i 的私钥，使得 $\{x_1, x_2, \cdots, x_n\}$ 是秘密值 $x \in Z_p^*$ 的 n 个秘密份额，并且任意 t 个或更多私钥的子集 SET 能通过拉格朗日插值方法重构 x. 设 U 的私/公钥对为 (x, y)，$x = \log_g y$. 每个 U_i 有它的私/公钥对 (x_i, y_i)，$y_i = g^{x_i}$ $(i = 1,2,\cdots,n)$. 算法 B 模拟随机算法 K_r. 敌手 A 能够获得参数 $\{I, y, y_r, y_i\}$ $(i = 1,2,\cdots,n)$.

令 $g_1 = g^a$，$g_2 = g^b$. 算法 B 随机选择两个数 $k^* \in Z_p^*$，$\beta \in Z_p^*$，对某个 $i \in Ind(U)$，计算 $c_{i1} = g^{k^*}$，计算 $g_3 = g_1^{-a^*} g^{\beta}$. 算法 B 替指定接收方 U_r 输出公钥 $y_r = \{g, g_1, g_2, g_3\}$.

攻击阶段 1. 敌手 A 适应性地作 DOLTAE 加解密预言机询问. 算法 B 像 DOLTAE 加密和解密在方案实际运行中的一样模拟 A 的视图.

DOLTAE 加密模拟. 当敌手 A 需要对一个消息 M 做 DOLTAE 加密时，A 甚至能按照门限策略指定一个特定的实际签名方群 $\mathcal{U}_a$. 不妨设 $\mathcal{U}_a$ 的基数是 t. 算法 B 先把明文 M 分成 t 个消息块. 对于所有 $i \in Ind(\mathcal{U}_a)$，算法 B 随机选择 $k_i \in Z_p^*$. 消息块 M_i 的序列号 n_i 和公钥 y 与 M_i 串联起来. 算法 B 对于所有 $i \in Ind(\mathcal{U}_a)$，如下计算消息块 M_i 的子密文：

$$\begin{aligned} & C_{i1} = g^{k_i}, \ \alpha_i = H_1(C_{i1}), \\ & C_{i2} = Z^{k_i}(n_i \| y \| M_i), \ C_{i3} = (g_1^{\alpha_i} g_3)^{k_i} \end{aligned} \tag{16}$$

$$s_i=H_2(y\|C_{i_11}\|C_{i_12}\|C_{i_13}\|\cdots\|C_{i_t1}\|C_{i_t2}\|C_{i_t3})^{L_ix_i} \tag{17}$$

最后，算法 B 把所有的子密文组合成消息 M 的 DOLTAE 密文：

$$s=\prod_{i\in Ind(\mathbf{U}_a)}s_i \tag{18}$$

算法 B 返回 DOLTAE 密文$(C_{i_11},C_{i_12},C_{i_13},\cdots,C_{i_t1},C_{i_t2},C_{i_t3},s)$作为 A 对 DOLTAE 加密询问的应答.

DOLTAE 解密模拟：当敌手 A 关于 DOLTAE 密文 $C=(C_{i_11},C_{i_12},C_{i_13},\cdots,C_{i_t1},C_{i_t2},C_{i_t3},s)$作解密随机预言机询问时，算法 B 作模拟应答.

1. 检查是否存在指标 i 使得 $C_{i1}=C_{i1}^*$ 或 $H_1(C_{i1})=H_1(C_{i1}^*)$. 如果存在，B 放弃.

2. 验证以下式子是否成立：

$$e(g,s)=e(y,H_2(y\|C_{i_11}\|C_{i_12}\|C_{i_13}\|\cdots\|C_{i_t1}\|C_{i_t2}\|C_{i_t3})) \tag{19}$$

如果不成立，B 返回⊥；否则，执行步 3.

3. 计算

$$\alpha_i^*=H_1(C_{i1}),\quad g_1^{k_{i1}}=(C_{i1}^{\beta}C_{i3}^{-1})^{1/(a^*-a)},$$
$$string_i^*=C_{i2}/e(g_1^{k_{i1}},g_2) \tag{20}$$

然后，B 把$string_i^*$分组为 $A_i^*\|B_i^*\|M_i^*$. 若 $A_i^*\notin Ind(\mathbf{U}_a)$，或者 $\exists i\neq j,A_i^*=A_j^*$，或 $\exists i,B_i^*\neq y$，B 返回⊥；否则，执行步 4.

4. 根据消息子块的序列号 A_i^*，B 把所有消息子块 M_i^* 拼接成整个消息 M.

挑战阶段. 敌手 A 选择两个长度相同的消息 M_0 和 M_1，把它们发送给算法 B. 算法 B 掷一个硬币决定 M_b，$b\in\{0,1\}$. 算法 B 如下计算 M_b 的 DOLTAE 密文 C 作为挑战challenge.

1. 把明文 M 分成 t 个消息块，选择某个 $i\in Ind(\mathbf{U}_a)$和随机数 $k^*\in Z_p^*$，计算

$$C_{i1}^*=g^{k^*},\ C_{i2}^*=Q^*(n_i\|y\|M_i),\ C_{i3}^*=(C_{i1}^*)^{\beta}.$$

2. 对于所有 $j\in Ind(\mathbf{U}_a)\backslash\{i\}$，B 做出与 DOLTAE 加密模拟类似的应答.

3. 返回一个挑战密文

$$Ch=(C_{i_11},C_{i_12},C_{i_13},\cdots,C_{i_t1},C_{i_t2},C_{i_t3},s).$$

攻击阶段 2. 敌手 A 以类似于攻击阶段 1 的方式适应性地发出加解密询问. 但不允许敌手 A 关于挑战 challenge Ch 询问解密随机预言机 $D_{sk_r}(\cdot)$.

猜测阶段. 在游戏结束时，A 输出一个比特 b'. 若 $b'=b$，则 A 赢得游戏.

下面通过归约方法来分析算法 B 成功的概率. A 发出各种随机预言机询问，算法 B 模拟 A 的视图. A 在模拟过程中的视图与 A 在实际协议运行中的视图几乎完全不可区分，除非以下事件发生.

事件 T_1. 当算法 B 对 DOLTAE 密文的解密询问做出应答时，若 $C_{i1}=C_{i1}^*$，则 B 放弃. 那么，对于 q_d 个解密询问，T_1 发生的概率是

$$Pr(T_1)\leq\frac{t}{p}+\frac{t}{p}+\cdots+\frac{t}{p-q_d+1}\leq\frac{2q_dt}{p} \tag{21}$$

事件 T_2. 当算法 B 对 DOLTAE 密文的解密询问做出应答时，若 $H_1(C_{i1})=H_1(C_{i1}^*)$，则 B 放弃. 若杂凑函数 $H_1()$的目标碰撞概率是 ε_1，则对 q_d 个解密询问，这个拒绝事件 T_2 发生的概率是

$$Pr(T_1)\leq t\varepsilon_1 \tag{22}$$

事件 T_3. 当敌手 A 选择消息，计算$(C_{i_11},C_{i_12},C_{i_13},\cdots,C_{i_t1},C_{i_t2},C_{i_t3},s)$，然后询问 DOLTAE 解密随机预言机时，B 无法对此解密询问作出正确的应答. 当且仅当以下式子成立时，事件 T_3 才发生：

$$e(g,s)=e(y,H_2(y\|C_{i_11}\|C_{i_12}\|C_{i_13}\|\cdots\|C_{i_t1}\|C_{i_t2}\|C_{i_t3})).$$

换言之，敌手 A 成功地了伪造一个 BLS 签名[22]. 因此，可以得到

$$Pr(T_2)=q_d\varepsilon_2 \tag{23}$$

事件 T_4. 除非攻击者 A 能区分 $e(g,g)^{abk^*}$ 和 G_2 中的一个随机元素，A 才能判断挑战密文的有效性. 攻击者 A 没有关于 b 的信息. 因此，可以得出

$$Pr(T_4)=1/2 \tag{24}$$

从以上式子(21)～(24)，可以得到

$$\varepsilon\leq Succ_{A,G_1}^{\mathrm{DBDH}}+\frac{2q_dt}{p}+t\varepsilon_1+q_d\varepsilon_2.$$

运行时间 t_1 和 t_2 是两个关于安全参数的概率多项式时间，具有相同的数量级. 因此，新的 DOLTAE 方案在 DBDH 假设下基于 RO 模型是 IND-CCA2 安全的.　　证毕.

定理 3(不可伪造性).　新的 DOLTAE 方案基于 CDH 假设在 RO 模型下是 UF-CTXT 安全的，并且有

$$\varepsilon_1\leq Succ_{A,G_1}^{\mathrm{CDH}}+\frac{q_h\cdot q_e}{p},$$

式子中 ε_1 是攻击者伪造 DOLTAE 密文的成功概率，$Succ_{A,G_1}^{\mathrm{CDH}}$ 是求解 CDH 问题成功的优势，q_h 是杂凑随机预言机访问的次数，q_e 是加密随机预言机访问的次数.

证明.　设 DOLTAE 方案为(K_c,K_s,K_r,E,D)，k 是系统安全参数. 假设存在(t_1,ε_1)攻击者 F，F 能够在时间 t_1 内以概率 ε_1 成功地对给定消息伪造有效的 DOLTAE 密文. 下面把新的 DOLTAE 方案的安全性归约到 CDH 假设. 为此需要应用 F 来构

造一个算法 A，该算法在时间 t_2 内以优势 $Succ_{A,G_1}^{CDH}$ 攻破 G_1 中的 CDH 假设.

给定 G_1 中的 CDH 问题实例：$\{g, g^{a^*}, g^{b^*}\}$，算法 A 的目标是计算 $g^{a^*b^*}$. 攻击者 F 能够访问签名随机预言机和随机杂凑预言机. F 预先选择多达 $t-1$ 个欲腐蚀的签名方. 不失一般性，假设 $\{\boldsymbol{U}_1^*, \boldsymbol{U}_2^*, \cdots, \boldsymbol{U}_{t-1}^*\}$ 是被 F 选定的欲腐蚀签名方群. 在 UF-CTXT 模型下，F 还能腐蚀接收者 U_r. 算法 A 通过攻击者 F 交互执行下列实验.

初始化阶段. 算法 A 运行算法 K_c. 输入安全参数 k，K_c 输出系统参数 $I=\{G_1, G_2, e, p, H_1(), H_2()\}$. F 甚至能够运行算法 K_r 来获得公/私密钥对 (pk_r, sk_r). A 模拟算法 K_s 和算法 K_r.

1. 将签名方群 $\mathbb{U}$ 的公钥 y 为挑战 g^{a^*}. 算法 A 在 Z_p^* 中随机选择 $t-1$ 个元素 $\{x_1', x_2', \cdots, x_{t-1}'\}$. 对于 $\{\boldsymbol{U}_1^*, \boldsymbol{U}_2^*, \cdots, \boldsymbol{U}_{t-1}^*\}$ 中每个签名方 $\boldsymbol{U}_i^*$，选定 x_i' 为它的私钥，则 $\boldsymbol{U}_i^*$ 的公钥是 $y_i'=g^{x_i'}$. 对于其他签名方，即 $j\notin Ind\{\boldsymbol{U}_1^*, \boldsymbol{U}_2^*, \cdots, \boldsymbol{U}_{t-1}^*\}$，A 计算 $y_j=\left(y\Big/\prod_1^{t-1} y_i^{L_i}\right)^{1/L_j}$. 上式中 Lagrange 系数 L_j 是与 L_i 通过指标集 $Ind\{\boldsymbol{U}_1^*, \boldsymbol{U}_2^*, \cdots, \boldsymbol{U}_{t-1}^*\}\cup\{j\}$ 计算的.

2. 在 Z_p^* 中随机选择 3 个元素 $\{a, b, c\}$. 计算 $g_1=g^a$，$g_2=g^b$，$g_3=g^c$，将他们作为指定接收方 U_r 的公钥.

3. 发送下列信息给 F：

$$\{I, y, (y_i', x_i'), y_j \mid i\in Ind\{\boldsymbol{U}_1^*, \boldsymbol{U}_2^*, \cdots, \boldsymbol{U}_{t-1}^*\}\}.$$

攻击阶段. F 适应性地发出随机杂凑预言机询问和 DOLTAE 加密随机预言机询问. A 模拟随机杂凑预言机和 DOLTAE 加密随机预言机的应答.

(1) 模拟随机杂凑预言机. 算法 A 创建两个杂凑值表 HL_1 和 HL_2. 表 HL_1 和 HL_2 分别用来存放 $H_1()$ 和 $H_2()$ 的值. 当 F 关于 C_{i1} 发出 $H_1()$ 询问时，A 在 Z_p^* 中随机选择一个元素 α_i，并把 (C_{i1}, α_i) 存放到 HL_1 中. 当 F 关于 $y\|C_{11}\|C_{12}\|C_{13}\|\cdots\|C_{t1}\|C_{t2}\|C_{t3}$ 发出 $H_2()$ 询问时，A 在 Z_p^* 中随机选择元素 d，计算 $(g^{b^*})^d$，把下列元组存放到 HL_2 中

$$(y\|C_{11}\|C_{12}\|C_{13}\|\cdots\|C_{t1}\|C_{t2}\|C_{t3}, d, (g^{b^*})^d).$$

(2) 模拟 DOLTAE 加密随机预言机. F 选择消息 M，关于 M 发出 DOLTAE 加密随机预言机询问. 实际签名方群甚至都可由 F 选定. 假设实际签名方群 $\mathbb{U}_a$ 是由 $\{\boldsymbol{U}_1^*, \boldsymbol{U}_2^*, \cdots, \boldsymbol{U}_{t-1}^*\}$ 和唯一诚实的签名方 U_j 组成. 对于这种选择，敌手 F 在作出 DOLTAE 加密询问时将有更多的优势. 对任意消息 M(M 不一定是新鲜的)，算法 A 如在新的 DOLTAE 方案中一样执行消息分块操作. 对于 $i\in Ind(\mathbb{U}_a)$，若 C_{i1} 以 (C_{i1}, α_i) 的形式出现在 HL_1 中，则令 $\alpha_i=H_1(C_{i1})$；否则，A 如在随机杂凑预言机模拟中一样进行模拟运算. 接着，A 计算 (C_{i2}, C_{i3}). 若列表 HL_2 中已经存在 $(y\|C_{11}\|C_{12}\|C_{13}\|\cdots\|C_{t1}\|C_{t2}\|C_{t3})$，则 A 终止模拟；否则，算法 A 随机选择一个元素 $d^*\in Z_p^*$，计算 g^{d^*}，存放 $(y\|C_{11}\|C_{12}\|C_{13}\|\cdots\|C_{t1}\|C_{t2}\|C_{t3}, d^*, g^{d^*})$ 到表 HL_2 中. 对于每个被腐蚀的签名方，算法 A 能通过式子(17)生成他们的 BLS 签名 s_i. 对于诚实签名方 U_j，A 计算 $s_j=y_j^{L_j d^*}$. 因为以下式子成立，s_j 一定是有效的.

$$e(g, s_j)=e(y_j, g^{L_j d^*})$$
$$=e(y_j, H_2(y\|C_{11}\|C_{12}\|C_{13}\|\cdots\|C_{t1}\|C_{t2}\|C_{t3}\|)^{L_j}).$$

算法 A 计算 $s=\prod_{i\in Ind(\mathbb{U}_a)} s_i$. 容易验证，下列式子成立：

$$e(g, s)=e(y, H_2(y\|C_{11}\|C_{12}\|C_{13}\|\cdots\|C_{t1}\|C_{t2}\|C_{t3})).$$

算法 A 能够完善地作出 DOLTAE 加密随机预言机的模拟.

密文伪造. 在实验结束时，攻击者 F 伪造认证密文 $(C_{11}, C_{12}, C_{13}, \cdots, C_{t1}, C_{t2}, C_{t3}, s)$. 这个伪造的密文不是 DOLTAE 加密随机预言机的输出.

输出. 算法 A 依照定义 9 中的方法验证伪造 DOLTAE 密文的有效性. 搜索表 HL_2，寻找到

$$(y\|C_{11}\|C_{12}\|C_{13}\|\cdots\|C_{t1}\|C_{t2}\|C_{t3}, d, (g^{b^*})^d).$$

这样，算法 A 能够计算出 $g^{a^*b^*}=s^{1/d}$.

下面用归约方法分析 F 的成功概率. F 在 A 模拟过程中的视图与在实际方案执行过程中的视图几乎完全不可区分. 除非在 DOLTAE 加密模拟时，$(y\|C_{11}\|C_{12}\|C_{13}\|\cdots\|C_{t1}\|C_{t2}\|C_{t3})$ 出现在表 HL_2 中，A 模拟失败. 这个事件发生的概率至多为 $\frac{q_h\cdot q_e}{p}$.

从以上讨论，可以得到

$$\varepsilon_1\le Succ_{A,G_1}^{CDH}+\frac{q_h\cdot q_e}{p},$$

$$t_2\le t_1+(n+4+1.5q_h+2.5q_e)T_e+(n-t-1)T_m,$$

上式中 T_e 与 T_m 分别指一次指数运算和乘法运算的时间.

在 DOLTAE 加密模拟过程中，没有要求消息 M 必须是新鲜的. 敌手伪造的密文所对应的消息可能是询问过 DOLTAE 加密随机预言机的消息，仅仅要求敌手伪造的密文不是 DOLTAE 加密随机预言机的应答. 因此，所提出的 DOLTAE 方案是 UF-CTXT 安全的. 证毕.

7 总　结

本文对 CHC-DOLTAE 方案[21]进行了分析，发现 CHC-DOLTAE 方案存在设计缺陷，以致于接收方无法恢复消息. 本文形式化了 DOLTAE 方案，构造了 DOLTAE 方案的形式化安全模型. 基于双线性映射，设计了一个新的 DOLTAE 方案. 在 CDH 与 DBDH 假设和随机预言机 RO 模型下，新的方案被证明对于适应性选择密文攻击是语义安全的，对于适应性选择消息攻击是存在性不可伪造的.

参　考　文　献

[1] Nyberg K, Rueppel R. A new signature scheme based on the DSA giving message recovery//Proceedings of the 1st ACM Conference on Computer and Communications Security. Fairfax, VA, 1993: 58-61

[2] Nyberg K, Rueppel R. Message recovery for signature schemes based on the discrete logarithm//Advances in Cryptology — EUROCRYPT'94. Berlin: Springer-Verlag, 1994: 175-190

[3] Horster P, Michels M, Petersen H. Authenticated encryption schemes with low communication costs. Electronics Letters, 1994, 30: 1212-1213

[4] Bellare M, Rogaway P. The exact security of digital signatures — How to sign with RSA and Rabin//Advances in Cryptology — Eurocrypt'96. LNCS 950. Berlin: Springer-Verlag, 1996: 399-416

[5] Bellare M, Namprempre C. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm//Advances in Cryptology — ASIACRYPT 2000. LNCS 1976. Berlin/Heidelberg: Springer, 2000: 531-545

[6] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) _ cost (signature) + cost (encryption)// Advances in Cryptology-CRYPTO'97. LNCS 1294. Berlin: Springer-Verlag, 1997: 165-179

[7] An J H. Authenticated encryption in the public-key setting: Security notions and analyses. Cryptology ePrint Archive: Report 2001/079. http: //eprint. iacr. org/2001/079

[8] Araki S, Uehara S, Imamura K. The limited verifier signature and its application. IEICE Transactions on Fundamentals, 1999, E82-A(1): 63-68

[9] Wu T S, Hsu C L. Convertible authenticated encryption scheme. Journal of Systems and Software, 2002, 62(3): 205-209

[10] Huang H F, Chang C C. An efficient convertible authenticated encryption scheme and its variant//Proceedings of the 5th International Conference on Information and Communications Security. LNCS 2836. Berlin: Springer-Verlag, 2003: 382-392

[11] Itakura K, Nakamura K. A public-key cryptosystem suitable for digital multi-signatures. NEC Research and Development, 1983, 71: 1-8

[12] Wu T S, Hsu C L, Tsai K Y, Lin H Y, Wu T C. Convertible multi-authenticated encryption scheme. Information Sciences, 2008, 178 (1): 256-263

[13] Tsai Jia-Lun. Convertible multi-authenticated encryption scheme with one-way hash function. Computer Communications, 2009, 32(5): 783-786

[14] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust threshold DSS signatures//Advances in Cryptology — Eurocrypt'96. LNCS 1070. Berlin, Heideberg: Springer-Verlag, 1996: 354-371

[15] Harn L. Group-oriented (t, n) threshold digital signature scheme and multi-signature. IEE Proceedings, Computers and Digital Techniques, 1994, 141(5): 307-313

[16] Chen Tzer-Shyong, Huang Kuo-Hsuan, Chung Yu-Fang. A division-of-labor-signature (t, n) threshold-authenticated encryption scheme with message linkage based on the elliptic curve cryptosystem//Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service, 2004: 106-112

[17] Lee W B, Chang C C. Authenticated encryption scheme without using a one way Function. Electronics Letters, 1995, 31(19): 1656-1657

[18] Lee W B, Chang C C. Authenticated encryption schemes with linkage between message blocks. Information Processing Letters, 1997, 63(5): 247-250

[19] Desmedt Y, Frankel Y. Threshold cryptosystems//Proceedings of the Advance in Cryptology — CRYPTO'89. LNCS 435. Berlin: Springer-Verlag, 1989: 307-315

[20] Tseng Y M, Jan J K. An efficient authenticated encryption scheme with message linkages and low communication costs. Journal of Information Science and Engineering, 2002, 18 (1): 41-46

[21] Chung Y F, Huang K H, Chen T S. Threshold authenticated encryption scheme using labor-division signature. Computer Standards & Interfaces, 2009, 31(2): 300-304

[22] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairings//Proceedings of the ASIACRYPT'01. LNCS 2248. Berlin: Springer, 2001: 514-532

[23] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 1987, 48(177): 203-209

[24] Lin C C, Laih C S. Cryptanalysis of Nyberg-Ruppel's message recovery scheme. IEEE Communication Letters, 2000, 4(7): 231-232

[25] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for discrete-log based cryptosystems//Stern J ed. Advances in Cryptology — Eurocrypt'99. LNCS 1592. Berlin: Springer-Verlag, 1999: 295-310

TAN Zuo-Wen, born in 1967, Ph.D., associate professor. His research interests include cryptography, information security.

FAN Yan-Fang, born in 1979, Ph. D. candidate. Her main research interests include computer security and security model.

Background

The research in this paper covers the formal division-of-labor threshold authenticated encryption (DOLTAE) scheme and its security model. The technique of division-of-labor can reduce the load of the signer group in the DOLTAE scheme. The threshold strategy can strengthen the security of authenticated encryption (AE) schemes. So the formalization of the DOLTAE scheme is necessary and important. The authors of this paper formalized the DOLTAE scheme and presented its formal security model. A novel DOLTAE scheme based on bilinear pairings is proposed. On the CDH and DBDH assumptions, the new scheme is proved to be semantic secure against chosen-ciphertext attacks (IND-CCA) and existential unforgeable with ciphertext forgery (UF-CTXT) against the adaptive chosen-message attacks in Random Oracle Model.

The research in this paper is supported by the National Natural Science Foundation of China under grant No. 10961013, which is related to the provable security issue of encryption schemes. Since security proof is a critical issue in the cryptographic protocol. So the research of the paper is important.

The main authors of this paper have gained sufficient archivement in terms of authenticated encryption (AE) schemes. Some related papers have been sent to some internation journals and some international conferences.

The achievement of this paper has solved the security issue and design of DOLTAE schemes in Random Oracle Model.